

Procedure - Auditing Protocol

Original Effective Date: 01/22/10	Revision Effective Date: 05/10/10, 05/21/12
-----------------------------------	---

1. Audit responsibility
 - a. Audits will be conducted by the participants as well as MS-HIN. The local care provider is most familiar with system use patterns.
 - b. Participating stakeholders (hospitals, clinics, FQHCs, etc.) should have a “designated” Auditor(s) to conduct routine auditing. MS-HIN also has a designated Auditor to assist with audit requests.
2. Audit Guidelines
 - a. MS-HIN will audit weekly random samples based on the evaluation criteria listed below.
 - b. MS-HIN recommends that each facility performs monthly audits of 5% of randomly selected patient charts.
 - Facility will monitor all provider accounts focusing on accounts of terminated or inactive employees. MS-HIN participants are responsible for deactivating User IDs of employees no longer with the organization.
 - MS-HIN will provide ongoing audit training services and support for clinic administrative users.
 - c. The auditor will run system audit reports to satisfy the following guidelines to monitor authorized user access to PHI information:

EVALUATION CRITERIA

- EXPANDED QUERY ACCESS - Monitor expanded query access: based on User, review User status and justification
 - o Received request for consultation
 - o Providing coverage for patient’s physician
 - o Patient is presenting for clinical care
 - o Patient is new to my practice
 - o Patient is presenting for emergency services
 - o I have a clinical relationship with this patient that is not yet established in MS-HIN
 - o For other payment or health operations
- LAST NAME MATCHING – Look for cases where individuals may be looking up relatives (same last name)
- REPEATED ACCESS TO SINGLE RECORD - Look for obvious pattern of excessive “hits” to single patient record
- DAY OF WEEK / TIME OF DAY - Look For: Time of access or break glass outside of work hours AND work location

- EMPLOYEE AS PATIENT - Monitor facility-specific employee or physician name searches if hospitalization information is known. NOTE: This audit is currently only being done only at the hospital facility level.
 - BUSINESS ASSOCIATE (BA) ACCESS - Look for BA access to records, administrative staff level access. Maintain a list of these users.
 - CHANGE IN JOB STATUS: Look for change in CE Workforce Job Status NOTE: This audit is currently being done only at the hospital participant level.
3. SPECIAL AUDITS – REQUESTED BY PARITICPANTS
- a. VIP/Sensational Audits
 - In the event of VIP care activity, a MS-HIN participant must notify the MS-HIN Office. Auditing shall occur for the record in addition to routine auditing. VIP care activity includes care of celebrities, executive staff leadership, high profile individual(s) in the media, etc. The MS-HIN participant will define VIP care activity.
 - b. Terminated Covered Entity (CE) Workforce
 - HOSPITAL PARTICIPANTS: The covered entity can notify MS-HIN to conduct an audit as needed.
 - CLINC/PROVIDER PARTICIPANTS: The covered entity is encouraged to notify MS-HIN to conduct an audit for a two week period prior to the password inactivation.
 - c. Change in Covered Entity (CE) Workforce Job Status
 - In the event a workforce member changes jobs and their MS-HIN ORG/User Role access has not been updated in a timely fashion and there was a change in access privileges, the CE can request a MS-HIN audit as needed.
 - d. Authenticate e-PHI status
 - In the event there is suspicion that e-PHI has been altered or destroyed in an unauthorized manner, the Covered Entity (CE) can notify MS-HIN who will in turn contact Medicity to provide detailed audit information for a specific MS-HIN record based on the specific incident. From there, next steps for addressing the incident and possible breach will be based on the audit findings.
4. Following HITECH guidelines, an ongoing report summarizing audit findings will be maintained by the MS-HIN Auditor.
5. If the auditing indicates suspicion of misuse based on specific information found during the weekly review:
- a. MS-HIN Auditor will document the finding and contact the provider/facility individually. The MS-HIN Director will assess the misuse in accordance with the ARRA/HITECH Act legislation guidelines, approved by the MS-HIN legal counsel. At minimum, access rights of the involved user party will be suspended based



on level of severity. (Further investigative action will be determined on a case-by-case basis, depending on the magnitude of the issue/situation.)

- b. MS-HIN Director will maintain internal reporting and detailed documentation of the reported incident.